ABSTRACT

An authentication protocol employs public-key computation to defeat denial-of-service attacks in a client-server system. The client enciphers and returns a random number chosen by the server to prove that it is legitimately participating in a service request, and not merely forcing the server to allocate resources to perform a request that will never be issued.